GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering

WEF Academic Year	: 2021-22
Semester	: 2
Category of the Course	: Program Core Course-IV
Course Name & Code	: Malware Analysis (4725902)

Prerequisite:

- Computer Organization - good understanding of instruction set architectures (registers, instruction encoding and decoding, and memory organization) and basic data types, data structures, function calls (calling conventions), and memory layout of programs.
- Ability to understand x86 and similar assembly; having a general understanding of computer security.
- OS fundamentals, fundamentals of C language.

Rationale:

- The course will focus on the fundamentals of malware and set up a protected static and dynamic malware analysis environment.
- The course will focus on the learning of various malware behaviour monitoring tools and actionable detection signatures from malware indicators.
- The course will focus on learning how to track malware into exhibiting behaviour that only occurs under special conditions.

Course Scheme:

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
03	00	02	04	70	30	30	20	150

Course Content:

Sr No	Course Content	No of Hours	%
1	**UNIT-I: Introduction:** Introduction to malware, OS security concepts, Malware threats, Evolution of malware, Malware types, Malware analysis types.	04	10%
2	UNIT-II: Virtual Machines and Emulators:	04	10%

	Benefits of virtualization, Oracle Virtual Box, VMware Player, Virtual PC, Open-source Alternatives: Bochs, QEMU, KVM.		
3	UNIT-III: Static Analysis: X86 Architecture- Main Memory, Instructions, Opcodes and Endian-ness, Operands, Registers, Simple Instructions, Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets, Anti-virus Scanning, Fingerprint for Malware, Portable Executable File Format, The PE File Headers and Sections, The Structure of a Virtual Machine, Reverse-Engineering- x86 Architecture, recognizing C code constructs in assembly, C++ analysis, Analyzing Windows programs, Anti-static analysis techniques: obfuscation, packing, metamorphism, polymorphism.	08	20%
4	UNIT-IV: Dynamic Analysis: Live Mal-ware analysis, dead Malware analysis, analyzing traces of Malware System-calls, API-calls, registries, network activities. Anti-dynamic analysis techniques: anti-vm, runtime-evasion techniques, Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching	08	15%
5	UNIT-V: Malware Functionality: Down-loaders, Back-doors, Credential Stealer's, Persistence Mechanisms, Privilege Escalation, Covert Malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.	06	15%
6	UNIT-VI: Malware Detection Techniques: Signature-based techniques: Malware signatures, packed Malware signature, metamorphic and polymorphic Malware signature non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences.	06	15%
7	UNIT-VII: Android Malware Analysis: Android Security Architecture, APK File Structure, Types of Mobile Malware, Malware Distribution Procedure, Malware Analysis of Malicious Mobile App., Reverse Engineering of Mobile App.	06	15%

Text Books/Reference Books:

1. "Practical malware analysis The Hands-On Guide to Dissecting Malicious Software" by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012
2. "Anti-Hacker Tool kit" by Mike Shema, Mcgraw Hill Education (India) Fourth Edition, 2014
3. "Hacking: The Art of Exploitation, 2nd Edition" by Jon Erickson.
4. "The IDA PRO Book: The Unofficial Guide to the World's Most Popular Disassembler, 2nd Edition" by Chris Eagle (published by No Starch Press, 2011).
5. "The GHIDRA Book: The Definitive Guide" by Chris Eagle and Kara Nance (Penguin Random House Publisher Services, 2020)
6. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006
7. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005
8. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010
9. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

Course Outcome:

After completion of the Course, Students will be able to:

No	Course Outcomes	RBT Level*
01	Understand the concept of the nature of malware, its capabilities and concepts of the virtual environment of the operating system.	UN
02	Apply the tools and methodologies used to perform static and dynamic analysis on the unknown executable.	AP
03	Execute techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.	AP
04	Analyze how malware interacts with any associated networks or devices, identifying the type of information being targeted.	AN
05	Monitor the Indicators of Compromise (IoCs) from malware samples to aid in threat intelligence efforts.	EL

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

Suggested Course Practical List:

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required:

- Course-related online MOOCs on NPTEL/SWAYAM/Coursera platform
- Recently Published papers/articles in reputed journals